Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Tuesday, November 21, 2006

Underappreciated (ii)

The potential for the application of discrete mathematics beyond computer science: in biology, economics, sociology, etc.

Hal Finney's Reusable Proofs of Work is important for at least two reasons: as a good stab at implementing bit gold, and for its use of the important idea of transparent servers: using remote attestation to verify the code running on servers.

The role of Stockholm syndrome in politics. Left as an exercise for the student. :-)

Three "silent" movies which I've had the good fortune to see on the big screen with live music: The Merry Widow, The Phantom of the Opera, and Safety Last.

Posted by Nick Szabo at 12:18 AM

2 comments:

Tony Finch said...

Proof-of-work does not work when people have widely differing computing capacities at their disposal. Since some of the world's largest distributed computing clusters are under the control of criminals, any cash based on how many gigaflops you have is doomed

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

to catastrophic fraud before it has even started.

2:48 AM

Nick Szabo said...

For applications like spam resistance using regular (not reusable) POW, your argument has some weight: to the extent these schemes assume spammers will exhaust their computing resources before end users, they may prove to be disillusioned.

But with respect to bit gold, you could make the same argument about gold and gold mines, and it would also be wrong. There are substantial economies of scale in gold mining and a handful of corporations are responsible for most of the world's gold mine output. That doesn't prevent a very competitive market in gold. (But see my comment on custom hardware below -- that is a scenario in which your argument has more weight).

For both gold and bit gold the price is determined by supply and demand. For both Hal's and my scheme the supply is determined by the scarcity at any given time. In Hal's scheme this is because tokens are turned over sequentially every time they are used and in my scheme because they are securely time-stamped. In my scheme later times will usually reflect lower computation costs and thus trade for a lower price, while in Hal's scheme the difficulty of the puzzle is gradually increased.

The worst problem, that I indicate in my article, is that somebody could come up with custom hardware with orders-of-magnitude advantage and possibly gain a near monopoly over the "mining" market until soembody else figures out a way to duplicate the hardware. This might or not beat the idea -- the market for time-stamped POW bits may adjust properly to even such a radical cost reduction -- but it's an important problem.

10:23 AM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ▼ 2006 (130)
  - ► December (4)
  - ▼ November (7)
    - Are most of us a bit Neanderthal?
    - Are green beards ubiquitous?
    - Underappreciated (ii)
    - Underappreciated
    - Towards smarter democracy
    - A raw idea to avoid being cooked
    - Robot law
  - ► October (15)
  - ► September (15)
  - ► August (20)
  - ► July (5)
  - ► June (10)
  - ► May (4)
  - ► April (3)
  - ► March (11)
  - ► February (10)
  - ► January (26)
- ► 2005 (44)

Simple theme. Powered by Blogger.